LISTING OF THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 Claim 1 (original): A method of testing a network firewall,
2 comprising:
3   transmitting a communications session initiation
4 signal from said signal source using an IP address
5 corresponding to said signal source to establish a
6 communications session to be conducted through said
7 firewall;
8   transmitting test signals from said signal source,
9 following initiation of said communications session and
10 prior to termination of said initiated communications
11 session, at a range of ports in a first side of said
12 firewall through which media signals may be transmitted
13 when said ports are open, said test signals including said
14 IP address;
15   monitoring a second side of said firewall to detect
16 any transmitted test signals that pass through said
17 firewall; and
18   identifying any open ports that are not associated
19 with said established communications session, which passed
20 at least one of said transmitted test signals, as
21 erroneously open ports.

1 Claim 2 (original): The method of claim 1, wherein said
2 transmitted test signals are IP packets which include said
3 IP address as a source address.

1 Claim 3 (original): The method of claim 1, further
2 comprising:

2

3   determining from at least one session initiation
4 signal at least one port associated with the established
5 communication session that should be open; and
6   generating an error signal indicating that said at
7 least one port associated with the established
8 communication session is erroneously closed if a test
9 signal is not detected passing through said port to the
10 second side of said firewall.

1 Claim 4 (original): The method of claim 3, further
2 comprising, prior to transmitting said communications
3 session initiation signal,
4   transmitting a first test signal at the first side of
5 said network firewall from the signal source using an IP
6 address that is not associated with any ongoing
7 communications session being conducted through said
8 firewall;
9   monitoring the second side of said firewall to
10 determine if said first test signal passed through said
11 firewall; and
12   reporting a firewall error if it is determined that
13 said first signal passed through said firewall.

1 Claim 5 (original): The method of claim 3, wherein said
2 transmitting steps are performed by a first test device and
3 said monitoring steps are performed by a second test
4 device, the second test device being physically separate
5 from said first test device, the method further comprising:
6   synchronizing the first and second test devices to a
7 common clock located external to said first and second test
8 devices.

3

1   Claim 6 (original): The method of claim 5, further
2   comprising;
3   operating the first test device to communicate
4   information identifying ports through which test signals
5   were detected passing through said firewall from the second
6   side to the second test device; and
7   operating the second test device to generate a test
8   report including information about the status of
9   unidirectional ports used to communicate signals from the
10 first side to the second side and unidirectional ports used
11 to communicate signals from the second side to the first
12 side.

1   Claim 7 (original): The method of claim 5, further
2   comprising;
3   operating the second test device to communicate
4   information identifying ports through which test signals
5   were detected passing through said firewall from the first
6   side to the first test device; and
7   operating the first test device to generate a test
8   report including information about the status of
9   unidirectional ports used to communicate signals from the
10 first side to the second side and unidirectional ports used
11 to communicate signals from the second side to the first
12 side.

1   Claim 8 (original): The method of claim 7, wherein said
2   session signal is at least one of SIP and H.323 compliant
3   signals.

1   Claim 9 (previously presented):   A firewall test system,
2   comprising:

4

3   a first test device located on an untrusted side of
4   said firewall, the first test device including:
5   i) a session signal generator for transmitting a
6   communications session initiation signal using an
7   IP address corresponding to said signal source to
8   establish a communications session to be
9   conducted through said firewall;
10   ii) a probe signal generator for generating test
11   signals at a range of ports in a first side of
12   said firewall through which media signals may be
13   transmitted when said ports are open, said test
14   signals including said IP address; and
15   iii) timing synchronization circuitry for
16   synchronizing said session signal generator and
17   said probe signal generator to at least one of
18   another test device and a clock signal source
19   located external to said first test device; and
20   a second test device located on a trusted side of said
21   firewall, the second test device including:
22   means for monitoring a second side of said
23   firewall to detect any transmitted test signals that
24   pass through said firewall; and
25   an analysis module for identifying any open
26   ports that are not associated with an established
27   communications session, which passed at least one of
28   said transmitted test signals, as erroneously open
29   ports.

1   Claim 10 (original):   The system of claim 9, wherein
2   said probe signal generator generates IP packets which
3   include said IP address as a source address.

5

1 Claim 11 (original):   The system of claim 9, wherein
2 said analysis module includes:
3   means for determining from at least one session
4 initiation signal at least one port associated with the
5 established communication session that should be open; and
6   means for generating an error signal indicating that
7 said at least one port associated with the established
8 communication session is erroneously closed if a test
9 signal is not detected passing through said port to the
10 second side of said firewall.

1 Claim 12 (original): The system of claim 11, wherein the
2 test signal generator of said first test device includes:
3   means for transmitting a first test signal at the
4 first side of said network firewall from the signal source
5 using an IP address that is not associated with any ongoing
6 communications session being conducted through said
7 firewall prior to said communications session initiation
8 signal being generated.

1 Claim 13 (original):The system of claim 11, wherein said
2 first test device further includes:
3   an analysis module for monitoring the second side of
4 said firewall to determine if said first test signal passed
5 through said firewall; and
6   a report generation module for reporting a firewall
7 error if it is determined that said first signal passed
8 through said firewall.

1   Claim 14 (original):The system of claim 9, wherein
2 said session signal generates at least one of SIP and H.323
3 compliant signals.

6